Scott Edward Cole, Esq. (S.B. #160744)
Laura Van Note Esq. (S.B. #310160)
Molly Munson Cherala, Esq. (S.B. #326195)
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com
Email: lvn@colevannote.com
Email: mmc@colevannote.com

Gary M. Klinger, Esq. (*pro hac vice*)
John J. Nelson, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
221 W Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: (866) 252-0878
Email: gklinger@milberg.com
Email: jnelson@milberg.com

Plaintiffs' Interim Co-Lead Class Counsel

Additional Counsel Listed on the Signature Page

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JOHN PRUTSMAN, AMIRA MARTZ, SIMCHA RINGEL, NAIOMI MARDEN, ALANA BALAGOT, CORINNE WARREN, SUNNY LAI, and DAVID KLEIN, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

NONSTOP ADMINISTRATION AND INSURANCE SERVICES, INC., inclusive,

Defendant.

Case No. 3:23-cv-01131-VC

CLASS ACTION

CONSOLIDATED AND AMENDED COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF

[JURY TRIAL DEMANDED]

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Plaintiffs John Prutsman, Amira Martz, Simcha Ringel, Naiomi Marden, Alana Balagot, Sunny Lai, Corinne Warren, and David Klein (collectively, "Plaintiffs") bring this Class Action Complaint against Nonstop Administration and Insurance Services, Inc. ("Defendant"), on behalf of themselves individually and all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII")[1] and protected health information ("PHI")[2] including, but not limited to, first, middle and last names, addresses, dates of birth, Social Security Numbers, medical record numbers, patient account numbers, driver's licenses and other government ID, healthcare provider's names and addresses, health plan names and health plan IDs, diagnoses, dates of services, treatment costs, prescription medications and numeric codes used to identify services and procedures (collectively "PHI/PII" or "PII and "PHI").

2. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Plaintiffs and, at least, 8,571 similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on December 22, 2022, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PHI/PII, which was being kept unprotected (the "Data Breach").[3]

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers etc.).

[2] Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[3] *Data Breach Portal https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf* (last accessed May 18, 2023).

3. Plaintiffs further seek to hold Defendant responsible for not ensuring that the PHI/PII was maintained in a manner consistent with industry standards, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards.[4]

4. While Defendant claims to have discovered the breach as early as December 22, 2022, Defendant did not begin informing victims thereof until February 22, 2023, and failed to inform victims when, first or for how long the Data Breach occurred. Indeed, Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it. For example, the Notice received by Plaintiff Sunny Lai was dated February 22, 2023. However, the other Plaintiffs, such as Alana Balagot, received notifications later. Ms. Balagot received her letter not until March 6, 2023.

5. Defendant acquired, collected and stored Plaintiffs' and Class Members' PHI/PII as part of providing health insurance services. Therefore, at all relevant times, Defendant knew or should have known that Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PHI/PII.

6. HIPAA establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans/insurers, healthcare clearinghouses and those healthcare providers that conduct certain healthcare transactions electronically and sets minimum standards for Defendant's maintenance of Plaintiffs' and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations like Defendant to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Plaintiffs' and Class Members' PHI/PII, including rights to examine and obtain copies of their health records and to request corrections thereto.

[4] Notably, Plaintiffs do not bring claims under HIPAA but, rather, allege that Defendant's failures to meet HIPAA standards serve as evidence of its negligence, generally.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of protected health information.

8. By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' PHI/PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles. Plaintiffs do not bring claims in this Action for direct violations of HIPAA but charge Defendant with various legal violations merely predicated upon the duties set forth in HIPAA.

9. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PHI/PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that sought to profit off this disclosure by defrauding Plaintiffs and Class Members in the future. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one other Class Member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

12. Defendant is headquartered and routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and/or services within this State.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiffs' claims took place within this District, and Defendant does business in this Judicial District.

PLAINTIFFS

Plaintiff John Prutsman

14. Plaintiff John Prutsman is an adult individual and, at all relevant times herein, a resident and citizen of Colorado, residing in Pagosa Springs, Colorado. Plaintiff Prutsman was notified of the Data Breach by a letter dated March 6, 2023.

15. As a result of the Data Breach, Plaintiff Prutsman lost time monitoring his credit scores and accounts. He also, inter alia, sustained emotional stress due to the Data Breach.

16. Plaintiff Prutsman has a continuing interest in ensuring that his PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Sunny Lai

17. Plaintiff Sunny Lai is an adult individual and, at all relevant times herein, a resident and citizen of California, residing in San Leandro, California. Plaintiff Lai was notified of the Data Breach by a letter dated February 22, 2023.

18. As a result of the Data Breach, Plaintiff Lai has had numerous fraudulent transactions on his accounts. Furthermore, Plaintiff Lai's credit score has dropped by more than 30 points. Inter alia, Plaintiff Lai has spent over twelve hours so far trying to remediate the damages due to the Data Breach.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

19. Plaintiff Lai has a continuing interest in ensuring his PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Amira Martz

20. Plaintiff Amira Martz is an adult individual and, at all relevant times herein, a resident and citizen of Alaska, residing in Wasilla, Alaska. Plaintiff Martz was notified of the Data Breach by a letter dated February 15, 2023.

21. As a result of the Data Breach, Plaintiff Martz received an alert that her information was available on the dark web. Plaintiff Martz immediately enrolled in credit monitoring and identify theft monitoring after the Data Breach to protect her information. Plaintiff Martz also placed credit freezes on her information as a result of the Data Breach. Inter alia, Plaintiff Martz has spent numerous hours trying to protect her PHI/PII as a result of the Data Breach.

22. Plaintiff Martz has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Simcha Ringel

23. Plaintiff Simcha Ringel is an adult individual and, at all relevant times herein, a resident and citizen of New York, residing in Brooklyn, New York. Plaintiff Ringel was notified of the Data Breach by a letter dated March 10, 2023.

24. As a result of the Data Breach, Plaintiff Ringel received a notification that his information was on the dark web. Inter alia, Plaintiff Ringel spent ten hours researching how his information was leaked on the dark web and how to best protect himself now that his PHI/PII had been exposed.

25. Plaintiff Ringel has a continuing interest in ensuring his PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

///

///

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Plaintiff Naiomi Marden

26. Plaintiff Naiomi Marden is an adult individual and, at all relevant times herein, a resident and citizen of California, residing in Oakland, California. Plaintiff Marden was notified of the Data Breach by a letter dated March 6, 2023.

27. As a result of the Data Breach, Plaintiff Marden had her accounts hacked including her credit monitoring account. Interalia, Plaintiff Marden has spent a significant amount of time changing her passwords and resetting her accounts as a result of the Data Breach.

28. Plaintiff Marden has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Alana Balagot

29. Plaintiff Alana Balagot is an adult individual and, at all relevant times herein, a resident and citizen of California, residing in Los Angeles, California. Plaintiff Balagot was notified of the Data Breach by a letter dated March 6, 2023.

30. As a result of the Data Breach, Plaintiff Balagot's PHI/PII was leaked onto the dark web. Plaintiff Balagot discovered a forum claiming to have possession of PHI/PII on the dark web. Inter alia, Plaintiff Balagot has spent over four hours monitoring her accounts and researching where her information ended up as a result of the Data Breach.

31. Plaintiff Balagot has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Corinne Warren

32. Plaintiff Corinne Warren is an adult individual and, at all relevant times herein, a resident and citizen of California, residing in Newark, California. Plaintiff Warren was notified of the Data Breach by a letter dated February 22, 2023.

33. As a result of the Data Breach, Plaintiff Warren has had three fraudulent credit inquiries according to TransUnion. Additionally, Plaintiff Warren had fraudulent applications opened in her name with Elon Financial Services. Inter alia, Plaintiff Warren has spent a significant

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

amount of time trying to monitor her accounts and protect herself from identity theft. Plaintiff Warren continues to suffer anxiety, stress, fear, frustration and sleep disruption as a result of the Data Breach.

34. Plaintiff Warren has a continuing interest in ensuring that her PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff David Klein

35. Plaintiff David Klein is an adult individual and, at all relevant times herein, a resident and citizen of New York, residing in Chappaqua, New York. Plaintiff Klein was notified of the Data Breach by a letter dated March 10, 2023.

36. As a result of the Data Breach, Plaintiff Klein has suffered an increase in spam calls, emails and texts. Plaintiff Klein has spent a significant amount of time remedying the harms caused by the Data Breach, including time spent communicating with financial institutions regarding fraudulent activity, contacting credit bureaus to place credit freezes on his accounts, and monitoring his accounts to protect himself from identity theft, which may take years to detect. In addition, Plaintiff Klein continues to suffer anxiety, stress, fear, frustration and sleep disruption as a result of the Data Breach.

37. Plaintiff Klein has a continuing interest in ensuring his PHI/PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

38. Defendant received highly sensitive PHI/PII from Plaintiffs in connection with the health insurance services. As a result, Plaintiffs' PHI/PII was among the data accessed by an unauthorized third party in the Data Breach.

39. At all times herein relevant, Plaintiffs are and were members of the National Class and each of their respective state Subclasses.

40. As required in order to obtain healthcare insurance services from Defendant, Plaintiffs provided Defendant with highly sensitive PHI/PII.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

41. Plaintiffs' PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Plaintiffs' PHI/PII. This PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

42. Each Plaintiff received a letter from Defendant stating that his/her PHI/PII was involved in the Data Breach (the "Notice").

43. As a result, Plaintiffs spent time dealing with the consequences of the Data Breach, which included and continues to include time, spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring accounts and seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

44. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PHI/PII—a form of intangible property that Plaintiffs entrusted to Defendant, which was compromised in and as a result of the Data Breach.

45. Plaintiffs suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling their PHI/PII.

46. Plaintiffs suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from their PHI/PII, in combination with their names, being placed in the hands of unauthorized third parties/criminals.

47. Plaintiffs have a continuing interest in ensuring that their PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

48. Defendant Nonstop Administration and Insurance Services is a California corporation with a principal place of business located at 1800 Center St., Suite 730, Concord, California 94520. Defendant Nonstop is a privately held, for-profit employee health insurance and benefits broker.[5]

[5] *About Us* https://www.nonstophealth.com/about-us/ (last accessed March 20, 2023)

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

49. Defendant provides healthcare insurance solutions nationwide. Previously, Nonstop Insurance and Administrative Services was only available to nonprofit organizations, but it has since expanded to be made available to a variety of organizations.[6]

50. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here, are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

51. Plaintiffs bring this class action pursuant to the provisions of Rules 23(a), 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure, on behalf of Plaintiffs and the following Classes and Subclasses (collectively, the "Class"):

Nationwide Class:
"All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or about December 22, 2022."

Alaska Subclass:
"All individuals within the State of Alaska whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or about December 22, 2022."

California Subclass:
"All individuals within the State of California whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or about December 22, 2022."

Colorado Subclass:
"All individuals within the State of Colorado whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or about December 22, 2022."

New York Subclass:
"All individuals within the State of New York whose PHI/PII was exposed to unauthorized third parties as a result of the data breach discovered by Defendant on or about December 22, 2022."

52. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded

[6] *Id.*

from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

53. Plaintiffs may request additional Subclasses as necessary based on the types of PHI/PII that were compromised.

54. Plaintiffs reserve the right to amend the above definitions or to propose Subclasses in subsequent pleadings and motions for class certification.

55. This action has been brought and may properly be maintained as a class action lawsuit under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Plaintiffs are informed and believe and, on that basis, allege that the total number of Class Members is in the thousands or tens of thousands of individuals. Membership in the Classes will be determined by analysis of Defendant's records.

b. Commonality: Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

1) Whether Defendant had a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws regulations, and industry standards relating to data security;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

6) Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their PHI/PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PHI/PII of Plaintiffs and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard the PHI/PII of Plaintiffs and Class Members;

11) Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Plaintiffs' claims are typical of the claims of the Plaintiff Classes. Plaintiffs and all members of the Plaintiff Class(es) sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Plaintiffs in this class action are adequate representatives of each of the Plaintiff Class(es) in that the Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class(es) in their entireties. Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Class(es) to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class(es), the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

56. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to individually bring all Class Members before the Court.

57. This Class Action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class and Subclasses in their entireties. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class and Subclasses in their entireties, not on facts or law applicable only to Plaintiffs.

58. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI/PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

59. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

60. On December 22, 2022, an unknown party contacted Defendant and stated that it had accessed Defendant's systems.[7] Nonstop allegedly investigated and confirmed that an unknown party had accessed Nonstop's cloud service platform.[8] In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data, including but not limited to, names, dates of birth, genders, physical and email addresses, telephone numbers, Social

[7] *Nonstop Health*, www.mass.gov/doc/assigned-data-breach-number-24318-nonstop-administration-and-insurance-services/download/ (last accessed May 18, 2023)

[8] *Id.*

Security numbers, medical treatment/diagnosis information and health insurance providers, claims and billing information. Plaintiffs were among the individuals whose data was accessed in the Data Breach.

61. Subsequent thereto, a hacking and data breach forum reported that 45,532 lines of data were posted online as a sample of the breach by cybercriminals.[9]

62. Plaintiffs were provided the information detailed above upon Plaintiffs' receipt of letters from Defendant. Plaintiffs were not aware of the Data Breach, or even that Defendant was still in possession of Plaintiffs' data, until receiving those letters.

Defendant's Failed Response to the Breach

63. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PHI/PII with the intent of engaging in misuse of the PHI/PII, including marketing and selling Plaintiffs' and Class Members' PHI/PII.

64. Not until roughly two months after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice provided only basic details of the Data Breach and Defendant's recommended next steps.

65. The Notice included, *inter alia*, the claims that Defendant had learned of the Data Breach on December 22, 2022 from an unknown party, and had taken steps to respond. However it did not state for how long the Data Breach occurred. The Notice claimed that Defendant implemented a redesigned cloud-services workflow and contacted law enforcement.[10]

66. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PHI/PII with the intent of engaging in misuse of the PHI/PII, including marketing and selling Plaintiffs' and Class Members' PHI/PII.

[9] *Nonstop Health data and source Code appear to have been leaked on hacking forum*, https://www.databreaches.net/nonstop-health-data-and-source-code-appear-to-have-been-leaked-on-hacking-forum/ (last accessed March 20, 2023).

[10] *Nonstop Health* www.mass.gov/doc/assigned-data-breach-number-24318-nonstop-administration-and-insurance-services/download (last accessed May 18, 2023)

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

67. Defendant had and continues to have obligations created by HIPAA, applicable federal and state law, as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiffs' and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

68. Plaintiffs and Class Members were required to provide their PHI/PII to Defendant in order to receive healthcare, and as part of providing healthcare insurance. Defendant created, collected, and stored Plaintiffs' and Class Members' PHI/PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

69. Despite this, Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PHI/PII going forward. Plaintiffs and Class Members are, thus, left to speculate as to where their PHI/PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

70. Plaintiffs' and Class Members' PHI/PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PHI/PII for targeted marketing without Plaintiffs' and/or Class Members' approval. Either way, unauthorized individuals can now easily access Plaintiffs' and Class Members' PHI/PII.

Defendant Collected/Stored Class Members' PHI/PII

71. Defendant acquired, collected, stored and assured reasonable security over Plaintiffs' and Class Members' PHI/PII.

72. As a condition of its relationships with Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PHI/PII. Defendant, in turn, stored that information of Defendant's system that was ultimately affected by the Data Breach.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

73. By obtaining, collecting and storing Plaintiffs' and Class Members' PHI/PII, Defendant assumed legal and equitable duties and knew or should have known that it was thereafter responsible for protecting Plaintiffs' and Class Members' PHI/PII from unauthorized disclosure.

74. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PHI/PII. Plaintiffs and Class Members relied on Defendant to keep their PHI/PII confidential and securely maintained, to use this information for business and healthcare purposes only and to make only authorized disclosures of this information.

75. Defendant could have prevented the Data Breach, which began as early as December 22, 2022, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiffs' and Class Members' PHI/PII.

76. Defendant's negligence in safeguarding Plaintiffs' and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

77. The healthcare industry has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25 percent increase.[11]

78. For example, Universal Health Services experienced a cyberattack on September 29, 2020 that appears similar to the attack on Defendant. As a result of this attack, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[12] Similarly, in 2021, Scripps Health suffered a cyberattack, an event which effectively shut down critical healthcare services for a month and left numerous

[11] *HIPAA Privacy Rule* https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed May 18, 2023).

[12] *Investor Overview* https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and (last accessed November 5, 2021).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

patients unable to speak to its physicians or access vital medical and prescription records.[13] A few months later, University of San Diego Health suffered a similar attack.[14]

79. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

80. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiffs' and Class Members' PHI/PII from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

81. In failing to adequately secure Plaintiffs' and Class Members' sensitive data, Defendant breached duties it owed Plaintiffs and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' PHI. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Plaintiffs' and Class Members' PHI/PII. Moreover, Plaintiffs and Class Members surrendered their highly sensitive PHI/PII to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their PHI/PII, independent of any statute.

82. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[13] *147,000+ May Have Had Personal Information Comprised in Cyberattack: Scripps Health* https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/ (last accessed May 18, 2023).

[14] *Data Breach at UC San Diego Health: Some Employee Email Accounts Impacted* https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/ (last accessed May 18, 2023).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

83. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

84. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

85. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

86. HIPAA's Security Rule required Defendant to do the following:

a. Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

87. HIPAA also required Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

88. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, required Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

89. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

90. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in Defendant's possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks and protocols adequately protected Plaintiffs' and Class Members' PHI/PII.

91. Defendant owed a duty to Plaintiffs and Class Members to design, maintain and test its computer systems, servers and networks to ensure that the PHI/PII in its possession was adequately secured and protected.

92. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PHI/PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

93. Defendant further owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

94. Defendant further owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

95. Defendant further owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII to Defendant.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

96. Defendant further owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

97. Defendant further owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identity possible threats.

Value of the Relevant Sensitive Information

98. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, prescriptions, treatment plans) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security Numbers and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

99. The high value of PHI/PII to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[16] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[17]

[15] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the- dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

100. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[18] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[19] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[20]

101. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

102. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

103. Identity thieves can use PHI/PII, such as that of Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture,

[18] *Healthcare Data Breaches: Insights and Implications* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed May 19, 2023).

[19] *December 2019 Healthcare Data Breach Report* https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed May 19, 2023).

[20] *Healthcare Security: Ransomware Plays a Prominent Role in COVID 19 Era Breaches* https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/ (last accessed May 19, 2023).

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

104. The ramifications of Defendant's failure to keep secure Plaintiffs' and Class Members' PHI/PII are long lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PHI/PII of Plaintiffs and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI/PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

105. There may be a time lag between when harm occurs versus when it is discovered, and also between when PHI/PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

106. The harm to Plaintiffs and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common and most expensive forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[22]

107. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[23]

[21] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed May 19, 2023).
[22] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed May 19, 2022).
[23] *Id*.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

108. When cybercriminals access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiffs and Class Members.

109. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[24] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[25]

110. And data breaches are preventable.[26] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[27] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[28]

111. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … "Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[29]

112. Here, Defendant knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Plaintiffs' and Class Members' PHI/PII was stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of

[24]See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed May 19, 2022).
[25]Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed May 19, 2023).
[26]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[27]*Id.* at 17.
[28]*Id.* at 28.
[29]*Id.* at 28.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols was necessary to fulfill its statutory and common law duties to Plaintiffs and Class Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

113. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class and all Subclasses)

114. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth herein

115. At all times herein relevant, Defendant owed Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Plaintiffs' and Class Members' PHI/PII in its computer systems and networks.

116. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in its possession;

b. to protect Plaintiffs' and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected its PHI/PII.

117. Defendant knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

118. Defendant knew or should have known of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

119. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PHI/PII.

120. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII that Plaintiffs and Class Members had entrusted to it.

121. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard the PHI/PII of Plaintiffs and Class Members.

122. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PHI/PII contained therein.

123. Plaintiffs' and Class Members' willingness to entrust Defendant with their PHI/PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PHI/PII it stored on them from attack. Thus, Defendant had a special relationship with Plaintiffs and Class Members.

124. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiffs and/or the remaining Class Members.

125. Defendant breached its general duty of care to Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

///

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard the PHI/PII of Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Plaintiffs' and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PHI/PII of Plaintiffs and Class Members, misuse the PHI/PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees to not store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class Members' PHI/PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

126. Defendant's willful failure to abide by these duties was wrongful, reckless and grossly negligent in light of the foreseeable risks and known threats.

127. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages.

128. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII to Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII.

129. Defendant breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiffs and Class Members, and then by failing and continuing to fail to provide Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and Class Members.

130. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PHI/PII, and to access their PHI/PII.

131. There is a close causal connection between Defendant's failure to implement security measures to protect the PHI/PII of Plaintiffs and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiffs and Class Members. Plaintiffs' and Class Members' PHI/PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing and maintaining appropriate security measures.

132. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

133. The damages Plaintiffs and Class Members have suffered, as alleged above, and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

134. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

135. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

136. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se.* Defendant also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

137. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in relation to its healthcare, (vii) the continued risk to their PHI/PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PHI/PII in their continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

138. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy, and other economic/non-economic losses.

139. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PHI/PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession.

/ / /

/ / /

/ / /

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Nationwide Class and all Subclasses)

140. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

141. Through its course of conduct, Defendant, Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PHI/PII.

142. Defendant required Plaintiffs and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendant's health insurance services.

143. Defendant solicited and invited Plaintiffs and Class Members to provide their PHI/PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PHI/PII to Defendant.

144. As a condition of being direct customers of Defendant, Plaintiffs and Class Members provided and entrusted their PHI/PII to Defendant. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if its data had been breached and compromised or stolen.

145. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PHI/PII to Defendant, in exchange for, amongst other things, the protection of their PHI/PII.

146. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

147. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

148. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered and will continue to suffer (a) ongoing,

imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (b) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (c) loss of the confidentiality of the stolen confidential data, (d) the illegal sale of the compromised data on the dark web, (e) lost time and (f) other economic/non-economic harm.

THIRD CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On behalf of the Nationwide Class and all Subclasses)

149. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

150. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs' and Class Members' PHI/PII, Defendant became a fiduciary by its undertaking and guardianship of the PHI/PII, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' PHI/PII; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

151. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PHI/PII.

152. Because of the highly sensitive nature of the PHI/PII, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PHI/PII had they known the reality of Defendant's inadequate data security practices.

153. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt, redact or otherwise protect Plaintiffs' and Class Members' PHI/PII.

154. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

155. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed supra).

FOURTH CLAIM FOR RELIEF
Declaratory Judgment
(On behalf of the Nationwide Class and all Subclasses)

156. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

157. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

158. An actual controversy has arisen in the wake of the data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PHI/PII and with regard to whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PHI/PII. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant surely denies these allegations. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their PHI/PII and remain at imminent risk that further compromises of their PHI/PII will occur in the future.

159. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, that:

a. Defendant continues to owe a legal duty to secure consumers' PHI/PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PHI/PII.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

160. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with the law and industry standards to protect consumers' PHI/PII.

161. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy in the event of another data breach affecting Defendant. The risk of another such breach is real, immediate and substantial. If another data breach affecting Defendant occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and/or quantifiable and because they will be forced to bring multiple lawsuits to rectify the same conduct.

162. The hardship to Plaintiffs and Class Members, if an injunction does not issue, exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs affecting Defendant, Plaintiffs and Class Members will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

163. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach affecting Defendant, thus eliminating the additional injuries that would result to Plaintiffs and the thousands of consumers whose confidential and valuable information would be further compromised.

FIFTH CLAIM FOR RELIEF
Alaska Consumer Protection Act
Alaska Stat. §§ 45.50.471, *et seq.*
(On behalf of the Alaska Subclass only)

164. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

165. The Alaska Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the Alaska Subclass, brings this claim.

166. Defendant advertised, offered or sold goods or services in Alaska and engaged in trade or commerce directly or indirectly affecting the people of Alaska.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

167. Alaska Subclass Members are "consumers" as defined by Alaska Stat. § 45.50.561(4).

168. Defendant engaged in unfair or deceptive acts and practices in the conduct of trade or commerce, in violation Alaska Stat. § 45.50.471, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or qualities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, when they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in any other conduct creating a likelihood of confusion or of misunderstanding which misleads, deceives or damages a buyer in connection with the sale or advertisements of its goods or services; and

e. Using or employing deception, fraud, false pretense, false promise, misrepresentation or knowingly concealing, suppressing or omitting a material fact with intent that others rely upon the concealment, suppression or omission in connection with the sale or advertisement of its goods or services whether or not a person was in fact misled, deceived or damaged.

169. Defendant's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Alaska Subclass Members' PHI/PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately maintain and/or improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Alaska Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Alaska Subclass Members' PHI/PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Alaska Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*;

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Alaska Subclass Members' PHI/PII; and

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Alaska Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*

170. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PHI/PII.

171. Defendant intended to mislead Plaintiff and Alaska Subclass Members and induce them to rely on its misrepresentations and omissions.

172. Defendant acted intentionally, knowingly and maliciously to violate Alaska's Consumer Protection Act and recklessly disregarded Plaintiff's and Alaska Subclass Members' rights.

173. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Alaska Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PHI/PII.

174. Plaintiff and the Alaska Subclass Members seek all monetary and nonmonetary relief allowed by law, including the greater of (a) three times their actual damages or (b) statutory damages in the amount of $500, punitive damages, reasonable attorneys' fees and costs, injunctive relief and any other relief that is necessary and proper.

SIXTH CLAIM FOR RELIEF
Alaska Personal Information Protection Act
Alaska Stat. §§ 45.48.010, *et seq.*
(On behalf of the Alaska Subclass only)

175. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

176. The Alaska Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the Alaska Subclass, brings this claim.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

177. Defendant is a business that owns or licenses PHI/PII, as defined by Alaska Stat. § 45.48.090(7). As such a business, it is a Covered Person as defined in Alaska Stat. § 45.48.010(a).

178. Plaintiff's and Alaska Subclass Members' PHI/PII includes Personal Information, as covered under Alaska Stat. § 45.48.010(a).

179. Defendant was required to accurately notify Plaintiff and Alaska Subclass Members if it became aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Alaska Stat. § 45.48.010(b).

180. Defendant is similarly required to determine the scope of the Data Breach and restore the reasonable integrity of the information system under Alaska Stat. § 45.48.010(b).

181. Because Defendant was aware of a breach of its security system, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Alaska Stat. § 45.48.010(b).

182. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Alaska Stat. § 45.48.010(b).

183. Pursuant to Alaska Stat. § 45.48.080(b), a violation of Alaska Stat. § 45.48.010(b) is an unfair or deceptive act or practice.

184. As a direct and proximate result of Defendant's violations of Alaska Stat. § 45.48.010(b), Plaintiff and Alaska Subclass Members suffered damages, as described above.

185. Plaintiff and Alaska Subclass Members seek relief measured as the greater of (a) each unlawful act, (b) three times actual damages in an amount to be determined at trial or (c) statutory damages in the amount of $500 for Plaintiff and each Alaska Subclass Member, reasonable attorneys' fees and any other just and proper relief available under Alaska Stat. § 45.48.080(b)(2) and Alaska Stat. § 45.50.531.

SEVENTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the California Subclass Only)

186. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

187. The California Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the California Subclass, brings this claim.

188. The State of California recognizes the tort of Invasion of Privacy both under the common law claim of intrusion upon seclusion and California's constitutional right to privacy.

189. Plaintiff and California Subclass Members had a legitimate expectation of privacy regarding their highly sensitive and confidential PHI/PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

190. Defendant owed a duty to its customers and their employees, including Plaintiff and California Subclass Members, to keep this information confidential.

191. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and California Subclass Members' PHI/PII is highly offensive to a reasonable person.

192. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and California Subclass Members disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and California Subclass Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

193. The Data Breach constitutes an intentional interference with Plaintiff and California Subclass Members interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

194. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

195. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and California Subclass Members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

196. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and California Subclass Members.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

197. As a proximate result of Defendant's acts and omissions, the private and sensitive PHI/PII of Plaintiff and California Subclass Members were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and California Subclass Members to suffer damages (as detailed *supra*).

198. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and California Subclass Members since their PHI/PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

199. Plaintiff and California Subclass Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PHI/PII of Plaintiff and California Subclass Members.

200. In addition to injunctive relief, Plaintiff, on behalf of themselves and the other California Subclass Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

EIGHTH CLAIM FOR RELIEF
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100, *et. seq.* ("CCPA")
(On Behalf of the California Subclass Only)

201. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

202. California Plaintiff Corinne Warren, individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the California Subclass, brings this claim.

203. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."

204. As a result, in 2018, the California Legislature passed the California Consumer Privacy Act (hereinafter "CCPA"), giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

205. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

206. Section 1798.150(a)(1) of the CCPA provides:

> "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper."

207. Plaintiff and California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

208. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; or annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

209. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and California Subclass Members' unencrypted first and last names and Social Security numbers among other information.

210. Plaintiff's and California Subclass Members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their Private Information, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

211. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and California Subclass Members' Private Information. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff's and California Subclass Members' PHI/PII as a result of this attack.

212. Pursuant to Section 1798.150(b) of the CCPA, on March 30, 2023, Plaintiff mailed written notice to Defendant of its violations of section 1798.150(a) by certified mail. *See* **Exhibit A**. Defendant responded to Plaintiff Warren's notice on April 11, 2023. *See* **Exhibit B**.

213. Defendant did not actually cure the noticed violations. Defendant asserted, without evidence or proof, that it "cured" the above failures to implement reasonable security procedures

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

to prevent unauthorized access of Plaintiff Warren's and California Subclass Members' PII by "enhance[ing] its already comprehensive security protocols." *Id*. These post- attack actions that Defendant allegedly took did not retroactively cure the unauthorized access, as they provide no assurance that Plaintiff Warren's and California Subclass members' PII was not viewed by—and/or is not still in the hands of—unauthorized third parties.

214. Furthermore, none of the steps Defendant assert in its response demonstrate an actual cure of its failure to implement reasonable security measures to protect Plaintiff Warren's and California Subclass Members' PII, as the steps they assert they have taken are not sufficient to protect Plaintiff Warren's and California Subclass Members' PII into the future.

215. Defendant's response is wholly insufficient to demonstrate any "actual cure" of its failure to implement reasonable security to protect Plaintiff Warren's and California Subclass Members' highly sensitive information.

216. As a result, Plaintiff Warren and the California Subclass seek relief under § 1798.150(a), including, but not limited to, statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

217. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

///

///

///

///

///

///

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

NINTH CLAIM FOR RELIEF
California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, *et seq*.
(On behalf of the California Subclass only)

218. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

219. Under California Civil Code § 56.06, Defendant is deemed a "provider of health care, health care service plan or contractor" and are, therefore, subject to the CMIA, California Civil Code §§ 56.10(a), (d) (e), 56.36(b), 56.101(a) and (b).

220. Under the CMIA, California Civil Code §56.05(k), California Plaintiff(s) (hereinafter "Plaintiff" for purposes of this Count only) and California Subclass Members, except employees of Defendant whose records may have been accessed, are deemed "patients."

221. As defined in the CMIA, California Civil Code § 56.05(j), Defendant disclosed "medical information" to unauthorized persons without obtaining consent, in violation of § 56.10(a). Defendant's misconduct, including failure to adequately detect, protect and prevent unauthorized disclosure, directly resulted in the unauthorized disclosure of Plaintiff's and California Subclass Members' PHI/PII to unauthorized persons.

222. Defendant's misconduct, including protecting and preserving the confidential integrity of their customers' PHI/PII, resulted in unauthorized disclosure of sensitive and confidential PHI/PII that belongs to Plaintiffs and California Subclass Members to unauthorized persons, breaching the confidentiality of that information, thereby violating California Civil Code §§ 56.06 and 56.101(a).

223. As a result of the Data Breach, unauthorized third parties viewed Plaintiff's and California Class Members' protected medical information.

224. Plaintiff and California Subclass Members have all been and continue to be harmed as a direct, foreseeable and proximate result of Defendant's breach because Plaintiffs and California Subclass Members face, now and in the future, an imminent threat of identity theft, fraud and for ransom demands. They must now spend time, effort and money to constantly monitor their accounts and credit to surveil for any fraudulent activity. Plaintiff and California Subclass

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Members were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their PHI/PII in violation of Cal. Civ. Code §§ 56.10 and 56.101 and, therefore, seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief and attorneys' fees and costs.

TENTH CLAIM FOR RELIEF
California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On behalf of the California Subclass only)

225. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

226. The California Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the California Subclass, brings this claim.

227. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

228. Defendant violated Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL") by engaging in unlawful, unfair and deceptive business acts and practices.

229. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members' PHI/PII from unauthorized disclosure, release, data breaches and theft, which was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks and adequately maintain and/or improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass Members, whose PHI/PII has been compromised.

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45, *et seq.*) and California's Consumer Records Act (Cal. Civ. Code § 1798.81.5).

c. Defendant's failure to implement and maintain reasonable security measures also leads to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

230. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and § 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, *et seq.* and California common law.

231. Defendant's unlawful, unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' PHI/PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately maintain and/or improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, and California's Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' PHI/PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, and California's Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*;

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass Members' PHI/PII; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*

232. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to

protect the confidentiality of consumers' PHI/PII.

233. As a direct and proximate result of Defendant's unfair, unlawful and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and lost money or property, including the price received by Defendant for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PHI/PII.

234. Defendant acted intentionally, knowingly and maliciously to violate California's Unfair Competition Law and recklessly disregarded Plaintiff's and California Subclass Members' rights.

235. Plaintiff and California Subclass Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful and fraudulent business practices or use of their PHI/PII, declaratory relief, reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5, injunctive relief and other appropriate equitable relief.

ELEVENTH CLAIM FOR RELIEF
California Customer Records Act
Cal. Civ. Code §§ 1798.80, *et seq*
(On behalf of the California Subclass only)

236. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

237. The California Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the California Subclass, brings this claim.

238. "[T]o ensure that PHI/PII about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification or disclosure."

239. Defendant is a "business" that owns, maintains and licenses Personal Information,

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass Members.

240. Businesses that own or license computerized data that includes Personal Information, including Social Security numbers, are required to notify California residents when their Personal Information has been acquired or is reasonably believed to have been acquired by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

241. Defendant is a "business" that owns or licenses computerized data that includes PHI/PII, as defined by Cal. Civ. Code § 1798.82.

242. Plaintiff's and California Subclass Members' PHI/PII includes Personal Information as covered by Cal. Civ. Code § 1798.82.

243. Because Defendant reasonably believed that California Plaintiffs' and California Subclass Members' PHI/PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

244. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

245. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members suffered damages, as described above.

246. Plaintiff and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

///

///

///

///

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

TWELFTH CLAIM FOR RELIEF
Colorado Security Breach Notification Act
Colo. Rev. Stat. §§ 6-1-716, *et seq.*
(On behalf of the Colorado Subclass only)

247. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

248. The Colorado Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the Colorado Subclass, brings this claim.

249. Defendant is a "business" that owns or licenses computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

250. Plaintiff's and Colorado Subclass Members' PHI/PII includes Personal Information, as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

251. Defendant was required to accurately notify Plaintiff and Colorado Subclass Members if it became aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

252. Because Defendant was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

253. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Colo. Rev. Stat. § 6-1-716(2).

254. As a direct and proximate result of Defendant's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass Members suffered damages, as described above.

255. Plaintiff and Colorado Subclass Members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

THIRTEENTH CLAIM FOR RELIEF
Colorado Consumer Protection Act
Colo. Rev. Stat. §§ 6-1-101, *et seq.*
(On behalf of the Colorado Subclass)

256. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

257. The Colorado Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the Colorado Subclass, brings this claim.

258. Defendant is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

259. Defendant engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

260. Plaintiff and Colorado Subclass Members, as well as the general public, are actual or potential consumers of the products and services offered by Defendant or successors in interest to actual consumers.

261. Defendant engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Knowingly making a false representation as to the characteristics of products and services;

b. Representing those services are of a particular standard, quality or grade, though Defendant knew or should have known that they were of another;

c. Advertising services with intent not to sell them as advertised; and

d. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

262. Defendant's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Colorado Subclass Members' PHI/PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately maintain and/or improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Colorado Subclass Members' PHI/PII, including by implementing and maintaining reasonable security measures;

///

///

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.;*

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Colorado Subclass Members' PHI/PII; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Colorado Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*

263. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PHI/PII.

264. Defendant intended to mislead Plaintiff and Colorado Subclass Members and induce them to rely on its misrepresentations and omissions.

265. Had Defendant disclosed to Plaintiff and Colorado Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as a large, sophisticated entity with the resources to put adequate data security protocols in place and as an organization that could be trusted with valuable PHI/PII regarding numerous consumers, including Plaintiff and the Colorado Subclass. Defendant accepted the responsibility while keeping the inadequate state of its security controls secret from the public. Accordingly, as Defendant held itself out as having the ability to maintain a secure environment for users' email accounts with a corresponding duty of trustworthiness and care, Plaintiff and the Colorado Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

266. Defendant acted intentionally, knowingly and maliciously to violate Colorado's Consumer Protection Act and recklessly disregarded Plaintiff's and Colorado Subclass Members' rights.

267. As a direct and proximate result of Defendant's deceptive trade practices, Colorado

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Plaintiff and Colorado Subclass Members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

268. Defendant's deceptive trade practices significantly impact the public, because nearly all members of the public are actual or potential consumers of Defendant's services and the Data Breach affected numerous individuals in the State of Colorado.

269. Plaintiff and Colorado Subclass Members seek all monetary and nonmonetary relief allowed by law, including the greater of (a) actual damages, (b) $500 or (c) three times actual damages for Defendant's bad faith conduct, injunctive relief and reasonable attorneys' fees and costs.

FOURTEENTH CLAIM FOR RELIEF
New York Information Security Breach and Notification Act
N.Y. Gen. Bus. Law § 899-aa
(On behalf of the New York Subclass only)

270. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

271. The New York Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the New York Subclass, brings this claim.

272. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a). Defendant also maintains computerized data that includes PHI/PII which Defendant does not own. Accordingly, it is subject to N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

273. Plaintiff's and New York Subclass Members' PHI/PII includes Private Information covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

274. Defendant is required to give immediate notice of a breach of security of a data system to owners of PHI/PII, including New York Plaintiff and New York Subclass Members, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

275. Defendant was required to accurately notify Plaintiff and New York Subclass Members if it discovers a security breach or receives notice of a security breach, which may have

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

compromised PHI/PII which Defendant owned or licensed, in the most expedient time possible and without unreasonable delay under N.Y. Gen. Bus. Law § 899-aa(2).

276. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

277. As a direct and proximate result of Defendant's violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiff and New York Subclass Members suffered damages, as described above.

278. Plaintiff and New York Subclass Members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

FIFTEENTH CLAIM FOR RELIEF
New York General Business Law
N.Y. Gen. Bus. Law §§ 349, *et seq.*
(On behalf of the New York Subclass only)

279. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth therein.

280. The New York Plaintiff(s), individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the New York Subclass, brings this claim.

281. Defendant engaged in deceptive acts or practices in the conduct of its business, trade and commerce or furnishing of services in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New York Subclass Members' PHI/PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately maintain and/or improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New York Subclass Members' PHI/PII, including by implementing and maintaining reasonable security measures;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*;

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New York Subclass Members' PHI/PII; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*

282. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PHI/PII.

283. Defendant acted intentionally, knowingly and maliciously to violate New York's General Business Law and recklessly disregarded Plaintiff's and New York Subclass Members' rights.

284. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PHI/PII.

285. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including numerous New Yorkers and New York businesses affected by the Data Breach.

286. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

287. Plaintiff and New York Subclass Members seek all monetary and nonmonetary relief allowed by law, including actual damages or statutory damages of $50 whichever is greater, treble damages, injunctive relief and attorney's fees and costs.

RELIEF SOUGHT

WHEREFORE, Plaintiffs, on behalf of themselves and each member of the proposed National Class and Subclasses, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declares, adjudges and decrees that this action is a proper Class Action and certifies each of the proposed Classes and/or any other appropriate subclasses under Federal Rules of Civil Procedure Rule 23 (b)(1), (b)(2) and/or (b)(3), including the appointment of Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal, triple and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoins Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PHI/PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

5. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;

c. requiring Defendant to delete and purge the PHI/PII of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PHI/PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Plaintiffs' and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiffs, individually, and on behalf of the Nationwide Class and Subclasses, hereby demand a trial by jury for all issues triable by jury.

Dated: May 25, 2023

COLE & VAN NOTE

By: */s/ Scott Edward Cole*
Scott Edward Cole, Esq.

Dated: May 25, 2023

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

By: */s/ Gary M. Klinger*
Gary M. Klinger, Esq.

Plaintiffs' Interim Co-Lead Class Counsel

Additional Counsel for Plaintiffs and Putative Class

M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
CLAYEO C. ARNOLD, A PROFESSIONALCORP
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Brittany Resch (*Pro Hac Vice*)
Raina Challeen Borrelli (*Pro Hac Vice*)
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
brittanyr@turkestrauss.com
raina@turkestrauss.com

Terence R. Coates
(*Pro Hac Vice* Forthcoming)
Dylan J. Gould (*Pro Hac Vice* Forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Exhibit A

ARNOLD LAW FIRM

865 Howe Avenue, Sacramento, CA 95825
7B Corporate Center Court, Greensboro, NC 27408
P: 916-777-7777 | F: 916-924-1829 | justice4you.com

CLAYEO C. ARNOLD
ANTHONY M. ONTIVEROS
JOHN T. STRALEN*
*The Board-Certified Civil Trial Advocate by the National Board of Trial Advocacy

M. ANDERSON BERRY
JOSHUA H. WATSON
ANDREW G. MINNEY
GREGORY HAROUTUNIAN
JEFFREY J.A. HINRICHSEN
BRANDON P. JACK
GINA M. BOWDEN**
**Of Counsel

CLASS ACTION
QUI TAM
DATA BREACH
PERSONAL INJURY
WRONGFUL DEATH
EMPLOYMENT LAW
PRODUCT LIABILITY

March 30, 2023

VIA FIRST CLASS MAIL

9489 0090 0027 6476 4630 48

Nonstop Administration and Insurance Services, Inc.
1800 Center Street, Suite 730
Concord, CA 94520

Nonstop Administration and Insurance Services, Inc.
c/o Agent Beck DeGeorge
CSC Lawyers Incorporating Service
2710 Gateway Oaks Drive
Sacramento, CA 95833

9489 0090 0027 6476 4630 31

RE: Statutory 30 Day Notice of Claim – Cal. Civil Code 1798.100, *et seq.*

This letter constitutes notice under the California Consumer Privacy Act ("CCPA"), California Civil Code §1798.100, *et seq*. Pursuant to Civil Code §1798.150(b), we are hereby notifying Nonstop Administration and Insurance Services, Inc. ("Nonstop") that it has violated the CCPA, and we demand that, to the extent any cure exists, Nonstop "actually cures" such violation within thirty (30) calendar days from the date of this letter.

Our client, Corine Warren, resident of San Francisco, California, received a Notice of Data Breach from Nonstop on or about February 22, 2023, stating that her personally identifiable information ("PII"), was accessed and no longer secure. The PII exposed includes, at least, her name, date of birth, Social Security number, and medical information. *See* CCPA §1798.81.5(d)(1).

Please be advised that the failure to prevent Ms. Warren's and other California residents' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure, is a result of Nonstop's failure to meet its duty to implement and maintain reasonable security procedures and practices, which is a violation of Civil Code §§ 1798.81.5, specifically § 1798.81.5(b), and 1798.150. These failures include, among other things, the lack of adequate encryption to sufficiently maintain California residents' PII and to protect this PII from being accessed by third parties without authorization.

To the extent there is any possible cure, we request that Nonstop cure this violation which exposed Ms. Warren's PII and provide an express written statement that the violations have been cured and that no further violations will occur. A cure, if possible, would require Nonstop to, for

example, recover all of the stolen PII and eliminate any future risk that Ms. Warren's stolen PII is misused.

A failure to comply with this request within thirty (30) calendar days will subject Nonstop to statutory damages on an individual and/or class-wide basis.

Thank you for your time and cooperation.

Very truly yours,

M. Anderson Berry, Esq.
aberry@justice4you.com
(916) 239-4778

MAB:lm

Exhibit B

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JILL H. FERTEL, ESQ.
Jfertel@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

Visit us online at
www.C-WLAW.com

April 11, 2023

M. Anderson Berry, Esq.
Arnold Law Firm
865 Howe Avenue, Sacramento, CA
7B Corporate Center Court
Greensboro, NC 27408
aberry@justice4you.com
via Electronic Mail

RE: Corine Warren – Statutory 30-Day Notice Under the California Consumer Privacy Act of 2018

Dear Mr. Berry:

This firm represents Nonstop Administration and Insurance Services, Inc. (hereinafter "Nonstop"). On **April 4, 2023**, our client received your Statutory Notice pursuant to the California Consumer Privacy Act of 2018 ("CCPA"). Specifically, your notice alleged that Nonstop failed to implement adequate security to maintain the personal identifying information ("PII") of California residents.

Initially, please be advised that the CCPA does not apply to Nonstop. The CCPA applies to for-profit businesses doing business in California that meet at least one of three criteria:

1. Has a gross annual revenue of over $25 million;
2. Buys, receives, or sells the personal information greater than or equal to that of 100,000 California residents, households, or devices; or
3. Derives 50% or more of their annual revenue from selling California residents' personal information.

Nonstop does not meet any of the criteria set forth above; the CCPA is therefore not applicable to Nonstop. Additionally, please note that all personally identifiable information ("PII") stored

within Nonstop's information systems was encrypted at the time of the breach and is thus further exempted by the statute.

Notwithstanding the inapplicability of the CCPA, Nonstop would offer the following response. Nothing in this correspondence shall however constitute an acceptance of application of the CCPA to Nonstop in this litigation or any other matter. Pursuant to Cal. Civ. Code. § 1798.150, Nonstop expressly states that, to the extent any potential violations of the CCPA exist, such violations have been cured. Specifically, Nonstop has enhanced its already comprehensive security protocols, including but not limited to the following:

Nonstop has retired its previous NSE production environment. Nonstop has rotated its database, cloud services, and access keys and forced password resets for internal Google access. Nonstop has implemented active security monitoring across all relevant accounts and networks. Nonstop has further created a new NSE administrative environment in a separate AWS account and implemented a Web Application Firewall on said environment and limited access exclusively to its corporate VPN; this VPN may only be accessed on company-owned machines. Nonstop uses new frameworks for securing application secrets and is rewriting applications to use password-less frameworks for database access. Moreover, Nonstop is refactoring document storage to preserve encryption at rest as well as during transport.

Additionally, a new NSE member environment has been created within a separate AWS account that has no access to the NSE administrative environment. The member application displays limited, non-sensitive personal information. Further security protocols were put in place with regards to member access to the NSE member environment including a separate web application firewall.

Nonstop has, and will continue to, employed security controls consistent with regulation and industry practices including wide use of encryption, penetration testing, phishing training and simulations and company-wide password protection.

Though this correspondence in no way constitutes an admission of liability, Nonstop asserts that any potential violation has been cured and expressly states that no future violations shall occur in the future.

Should you have any additional questions or concerns, please do not hesitate to contact me.

Sincerely,

/s/ Jill H. Fertel

CERTIFICATE OF SERVICE

I hereby certify that, on May 25, 2023, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify the foregoing document is being served today on all counsel of record in this case via transmission of Notice of Electronic Filing generated by CM/ECF and on counsel in the related cases to their respective emails per the below service list.

/s/ Scott Edward Cole
Scott Edward Cole, Esq.